

This Page Is Inserted by IFW Operations  
and is not a part of the Official Record

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

**IMAGES ARE BEST AVAILABLE COPY.**

As rescanning documents *will not* correct images,  
please do not report the images to the  
Image Problem Mailbox.

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-139735

(43)Date of publication of application : 27.05.1997

(51)Int.Cl.

H04L 9/08  
G06F 15/00  
G09C 1/00  
G09C 1/00

(21)Application number : 07-297026

(71)Applicant : HITACHI SOFTWARE ENG CO LTD

(22)Date of filing : 15.11.1995

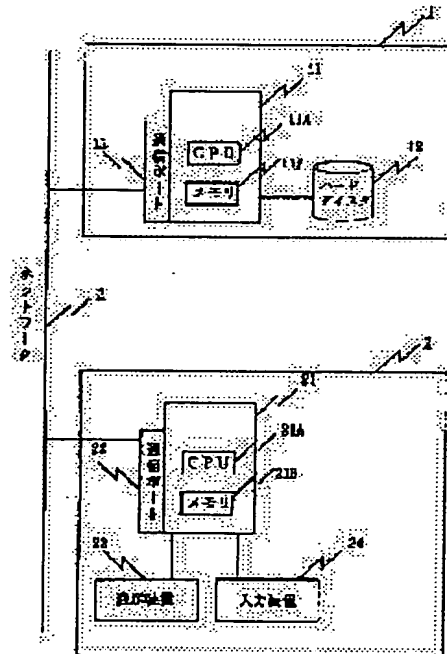
(72)Inventor : FUJIOKA HIDEKI

## (54) CIPHERING DATA COMMUNICATION SYSTEM

## (57)Abstract:

PROBLEM TO BE SOLVED: To secure security of data communication by incorporating a relay service program to realize ciphering data communication to memories of a server and a client, respectively.

SOLUTION: A server 1 and a client 2 are connected via a network 3. A relay service program to realize ciphering data communication is incorporated in memories 11B, 21B of the server 1 and the client 2. Thus, an application program of its own computer ciphers data to be sent to an application program of other computer. Then data received from the application program of the other computer are decoded and given to the application program of its own computer.



## LEGAL STATUS

[Date of request for examination] 18.06.1998

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2000 Japanese Patent Office

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平9-139735

(43)公開日 平成9年(1997)5月27日

(51)Int.Cl. <sup>6</sup>	識別記号	庁内整理番号	F I	技術表示箇所
H 0 4 L 9/08			H 0 4 L 9/00	6 0 1 B
G 0 6 F 15/00	3 3 0		G 0 6 F 15/00	3 3 0 B
G 0 9 C 1/00	6 3 0	7259-5 J	G 0 9 C 1/00	6 3 0 B
	6 6 0	7259-5 J		6 6 0 E

審査請求 未請求 請求項の数 3 O L (全 12 頁)

(21)出願番号 特願平7-297026

(22)出願日 平成7年(1995)11月15日

(71)出願人 000233055

日立ソフトウェアエンジニアリング株式会  
社

神奈川県横浜市中区尾上町6丁目81番地

(72)発明者 藤岡 秀樹

神奈川県横浜市中区尾上町6丁目81番地

日立ソフトウェアエンジニアリング株式会  
社内

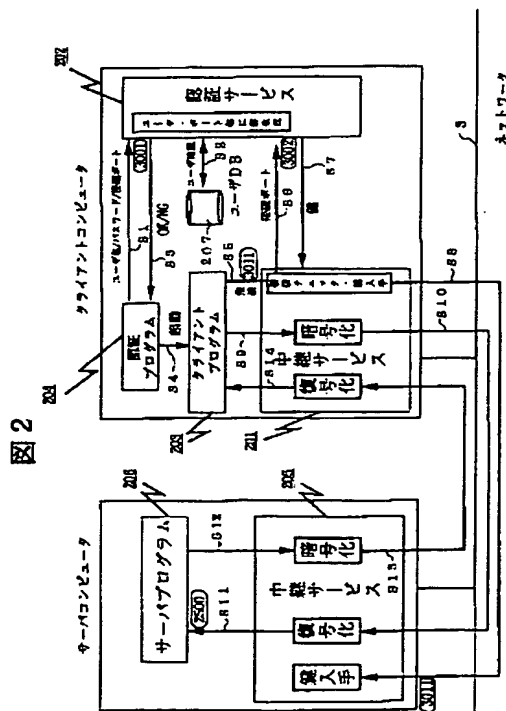
(74)代理人 弁理士 秋田 収喜

(54)【発明の名称】 暗号化データ通信システム

(57)【要約】

【課題】 既存のアプリケーションやオペレーティングシステムに変更を加えることなく、ネットワーク上を流れるデータを暗号化し、データ通信のセキュリティを確保する。

【解決手段】 2つのコンピュータ上で、それぞれ中継サービスプログラムを稼動させておき、この中継サービスでデータを暗号化させ、ネットワーク経由で送受信する。



**【特許請求の範囲】**

**【請求項1】** ネットワーク経由でデータを通信する少なくとも2つのコンピュータを備えた暗号化データ通信システムであって、前記各コンピュータは、自コンピュータのアプリケーションプログラムが他方のコンピュータのアプリケーションプログラムに送信するデータを暗号化し、他方のコンピュータのアプリケーションプログラムから受信したデータを復号し、自コンピュータ内のアプリケーションプログラムに渡す中継サービス処理手段を備えることを特徴とする暗号化データ通信システム。

**【請求項2】** 前記各コンピュータは、自コンピュータのアプリケーションプログラムがデータを通信する際に、該アプリケーションプログラムを使用するユーザの認証処理によってユーザ毎の暗号鍵を生成し、中継サービス処理手段に転送する認証処理手段をさらに備えることを特徴とする請求項1記載の暗号化データ通信システム。

**【請求項3】** 前記中継サービス処理手段は、所定の記録媒体に記録されたプログラムとして各コンピュータ内に組み込まれるものである請求項1または2記載の暗号化データ通信システム。

**【発明の詳細な説明】****【0001】**

**【発明の属する技術分野】** 本発明は、ネットワークに接続された複数のコンピュータ間でデータの送受信を行う際に、既設のオペレーティングシステムや通信用プログラムに変更を加えることなく、クライアントコンピュータとサーバコンピュータ間で通信されるデータのセキュリティを確保するための暗号化データ通信システムに関するものである。

**【0002】**

**【従来の技術】** コンピュータの性能の向上、ネットワークへの接続が進むにつれ、情報を複数のコンピュータに分散させて保存し、ネットワークに接続している別のコンピュータから参照するという分散コンピューティングが行われてきている。

**【0003】** このように、ネットワークに接続されたコンピュータ間で情報をやり取りする場合、サーバ・クライアント型の形態で情報通信を行うが、この時ネットワーク上には情報がそのまま流れるため、人事情報や企業間での情報のやり取りを行った場合、傍受される危険性が高い。

**【0004】** そこで、従来は、これを防ぐために、

(1) 一旦暗号化した情報を電子メールやファイル転送で配送する、(2) セキュリティルータに代表される暗号化機能を持ったハードウェアを利用し、ルータ間で暗号化した情報を転送する、(3) 「Kerberos」のように、オペレーティングシステム自身にセキュリティ機能を持たせ、通信時のセキュリティを確保する、な

どの方策が実施されている。

**【0005】** また、特開平3-80752号公報に開示されているように、端末が交換機に直接接続されている場合に、別の交換機に接続された端末間での通信を傍受されないように、交換機内に暗号化機能を付加したものがある。

**【0006】**

**【発明が解決しようとする課題】** しかしながら、前記(1)の方法でデータを通信するシステムにあつては、データ自身の暗号化は通信用プログラムと全く別の部分で行うか、またはサーバコンピュータやクライアントコンピュータ上で動作する通信用プログラム内に暗号化機能を組み込む必要がある。しかし、通信用プログラムと全く別の部分(暗号化プログラム)で暗号化するようにした場合、既設の通信用プログラムの中に暗号化プログラムを呼び出す処理を追加しなければならなくなり、一般ユーザにおいては実現不可能である。また、通信用プログラム内に暗号化機能を組み込むようにした場合、アプリケーション開発者にとって負担が大きいという問題がある。

**【0007】** 次に、(2)の方法でデータを通信するシステムにあつては、ルータ間のセキュリティは確保されているが、ルータ内のネットワーク上には「生のデータ」が流れるため、通信のセキュリティを確保することはできない。

**【0008】** この場合、サーバコンピュータやクライアントコンピュータ内に、暗号化機能を実現するハードウェアを追加することが考えられるが、ハードウェアの追加空間が常に確保されているとは限らず、追加空間が無い場合は通信のセキュリティを確保することはできない。さらに、追加空間があったとしても、前記(1)の場合と同様に、既設の通信用プログラムの中に暗号化用ハードウェアを呼び出す処理を追加しなければならなくなり、一般ユーザにおいては実現不可能である。

**【0009】** 次に、(3)の方法でデータを通信するシステムにあつては、全ての通信にセキュリティが確保されるが、全てのコンピュータのオペレーティングシステムがセキュリティ機能を装備していることが必要になり、既存のオペレーティングシステムを利用したアプリケーションには適用できないという問題がある。

**【0010】** さらに、特開平3-80752号公報に開示されている方法でデータを通信するシステムにあつては、汎用計算機の端末などで扱うデータを電話回線を通じて中央の汎用計算機に一旦集めた後に転送する場合には利用可能であるが、1本の伝送媒体に複数のコンピュータが接続されているバス形式のネットワークの形態である場合、ネットワーク上に「生のデータ」が流れるため、通信のセキュリティが確保できないという問題がある。

**【0011】** 本発明の目的は、既設または既存のアプリ

ケーション（通信用プログラムなど）やオペレーティングシステムに全く変更を加えずに、全ての接続形態のネットワーク上で通信されるデータのセキュリティを確保することができる暗号化データ通信システムを提供することにある。

#### 【0012】

【課題を解決するための手段】本発明は、上記目的を達成するために、ネットワーク経由でデータを通信する各コンピュータ内に、自コンピュータのアプリケーションプログラムが他方のコンピュータのアプリケーションプログラムに送信するデータを暗号化し、他方のコンピュータのアプリケーションプログラムから受信したデータを復号し、自コンピュータ内のアプリケーションプログラムに渡す中継サービス処理手段を設けたことを特徴とする。

#### 【0013】

【発明の実施の形態】以下、本発明の実施の形態を図面を用いて詳細に説明する。

【0014】図1は、本発明を適用した暗号化データ通信システムの実施形態の一例を示すシステム構成図である。

【0015】この実施形態は、データのセキュリティを必要とする「社員の健康管理業務」を行う健康管理システムを想定して構成されている。健康管理業務では、社員のプライバシーに関する情報を扱うため、ネットワークに流れるデータを傍受から守るために、暗号化によって通信セキュリティを確保することが必須である。

【0016】この実施形態のシステムは、ネットワーク3で接続されたサーバコンピュータ1とクライアントコンピュータ2とで構成されている。

【0017】サーバコンピュータ1は、CPU11A、メモリ11Bから成る端末装置11と、社員の健康管理情報を保存しておくための外部記憶装置12と通信ポート13とを備えている。

【0018】クライアントコンピュータ2は、サーバコンピュータ1と同様に、CPU21A、メモリ21Bからなる端末装置21と、通信ポート22、健康管理データベースの検索結果などを表示する表示装置23、及び健康管理システムを起動するためにユーザ名称やパスワードを入力したり、あるいは健康管理データベースへの検索指示を入力する入力装置24とを備えている。

【0019】これらサーバコンピュータ1およびクライアントコンピュータ2のメモリ11A、11Bには、暗号化データ通信を実現するための中継サービスプログラムが組み込まれている。この中継サービスプログラムは、フロッピディスクまたはCD-ROM、またはICカードなどの記録媒体によってサーバコンピュータ1およびクライアントコンピュータ2のユーザに提供されるもので、起動プログラムによって稼働状態にしたり、非稼働状態にすることができる。非稼働状態にした場合

は、暗号化機能は停止される。また、中継サービスプログラムは、前記のような記憶媒体でなく、ネットワーク内の上位コンピュータあるいはサーバコンピュータからダウンロードする形式でユーザに提供される。

【0020】図2は、中継サービスプログラムを利用してサーバコンピュータ1とクライアントコンピュータ2との間で通信を行う際のデータの流れを示したものである。

【0021】データ転送のためのプロトコルとしては様々なものが利用可能であるが、本実施例ではTCP/IPを利用する。TCP/IPでは、各コンピュータごとに、そのコンピュータ上で稼働するサービスプログラムが通信に使用するために、ポートと呼ばれる番号を持っている。

【0022】クライアントコンピュータ1では、中継サービスプログラム201と、認証サービスプログラム202が稼働している。

【0023】一方、サーバコンピュータ2では、中継サービスプログラム205と社員の健康管理情報を格納したデータベースを処理するサーバプログラム206が稼働している。

【0024】ユーザは、健康管理システムを実現するためのクライアントプログラム203を起動する際に、必ず認証プログラム204を起動する。認証プログラム204は、クライアントコンピュータ2の表示装置上にユーザ名称とパスワードの入力を促す画面を表示する。

【0025】ユーザが健康管理システムを使用するために、ユーザ名称とパスワードを入力すると、認証プログラム204は、認証サービスプログラム202のサービスポートである「3001番」に対して接続し、ユーザ名、パスワードとクライアントプログラム203が中継サービスプログラム201のどのポートに接続するかを示すポート番号を転送する（S1）。

【0026】これに対し、認証サービスプログラム202は、ユーザ名称とパスワードを利用してユーザDB207に対してユーザ確認を行う（S2）。

【0027】その結果、ユーザがユーザDB207に予め登録されている正規の利用者であると認証された場合は、認証サービスプログラム202は「OK」を、認証されない場合は「NG」を認証プログラム204に返答する（S3）。

【0028】認証プログラム204は、認証結果が「NG」の場合は再度ユーザ名とパスワードの再入力を促す画面を表示する。認証結果が「OK」の場合は、認証プログラム204はクライアントプログラム203を起動する（S4）。

【0029】クライアントプログラム203は、中継サービスプログラム201の通信ポートである「3011番」に対して接続する（S5）。

【0030】中継サービスプログラム201は、認証サ

ービスプログラム202の暗号鍵通信ポートである「3002番」に接続し、クライアントプログラム203から接続されたポート番号を認証サービスプログラム202に渡し(S6)、そのポート番号で認証されたユーザの暗号鍵を入手する(S7)。

【0031】その後、中継サービスプログラム201は、サーバコンピュータ1で稼働している中継サービスプログラム205の中継ポートである「3011番」

「に接続し、認証サービスプログラム202から入手した暗号鍵を中継サービスプログラム201、205に固有の鍵で暗号化して中継サービスプログラム205にネットワーク3経由で送信する。

【0032】サーバコンピュータ1の中継サービスプログラム205は、クライアントコンピュータ2の中継サービスプログラム201から送信されてきた「暗号化された暗号鍵」を中継サービス固有の鍵で復号し保持しておく(S8)。

【0033】クライアントプログラム203は、サーバプログラム206に送信すべきデータを中継サービスプログラム201に送信する(S9)。

【0034】送信するデータには、サーバコンピュータ側のデータベースのアクセス許可を得るためのユーザ名称とパスワードや、データベース検索のためのSQL文などがあり、これらは通常のテキスト形式で送信される。

【0035】中継サービスプログラム201は、クライアントプログラム203から送信されてきたデータを、認証サービスプログラム202から入手した暗号鍵で暗号化し、サーバコンピュータ1の中継サービスプログラム205に転送する(S19)。

【0036】中継サービスプログラム205は、サーバプログラム206の受信ポートである「2500番」に接続し、クライアントコンピュータ2の中継サービスプログラム201から受信したデータを、保持しておいた暗号鍵で復号し、サーバプログラム206に送信する(S11)。

【0037】サーバプログラム206は、受信したデータを処理した後、結果を中継サービスプログラム205に送信する(S12)。

【0038】中継サービスプログラム205は、受信したデータを、保持しておいた暗号鍵で暗号化し、クライアントコンピュータ2の中継サービスプログラム201に送信する(S13)。

【0039】クライアントコンピュータ2の中継サービスプログラム201は、受信したデータを、保持しておいた暗号鍵で復号し、クライアントプログラム203に転送する(S14)。

【0040】このようにうして、健康管理システムであるクライアントプログラム203がサーバプログラム206から受け取るデータは、クライアントプログラム2

03がサーバプログラム206と直接通信して得られるデータと全く等しいものである。

【0041】以後、クライアントプログラム203とサーバプログラム206の間の通信は、上記の手順S9～S14を繰り返すことにより、クライアントコンピュータ2とサーバコンピュータ2上で稼働する中継サービスプログラム201、205を経由して行われる。

【0042】図4は、認証プログラム204の動作を示すフローチャートである。

【0043】以下、図4のフローチャートを用いて、本実施例の動作を説明する。

【0044】まず、表示装置上に、暗号化中継サービスを経由して稼働するシステム名の選択画面を表示する(ステップ301)。この利用システムの選択画面401には、図4に示すように、暗号化中継サービスを経由して稼働するシステム名が複数個表示される。ユーザは、この中の1つ、例えば「健康管理システム」402をカーソル移動によって選択する。

【0045】なお、暗号化中継サービス自体も図4の選択画面401で選択する。図4においては、既に暗号化中継サービスが選択され、次に健康管理システムを選択した状態を示している。

【0046】次に、認証プログラム204は、ユーザ名称とパスワードを入力する画面を表示する(ステップ302)。この入力画面501には、図5に示すように、ユーザ名称502とパスワード503の入力エリアが表示される。ユーザは、これらの入力エリアにユーザ名称502とパスワード503を入力する。

【0047】次に、認証プログラム204は、ユーザから入力されたユーザ名称502とパスワード503を取り込む(ステップ303)。この後、認証サービスプログラム202に接続し(ステップ304)、取り込んだユーザ名称502とパスワード503のペアと、認証後に起動するクライアントプログラム(健康管理システム)203が中継サービスプログラム201に接続する時のTCP/IPポートを認証サービスプログラム202に送信する(ステップ305)。

【0048】次に、認証サービスプログラム202から認証の結果を受信する(ステップ306)。そして、受信した結果をチェックし(ステップ307)、「NG」であれば、ステップ303から繰り返す。「OK」であれば、クライアントプログラム(健康管理システム)203を起動し(ステップ308)し、終了する。

【0049】図6は、認証サービスプログラム202の動作を示すフローチャートである。

【0050】まず、認証サービスプログラム202は、クライアントコンピュータ2のユーザDB207内に設けられ、ユーザ名称とパスワードのペアを格納しているファイルを開き、その内容をメモリ中に読み込む(ステップ601)。

【0051】次に、TCP/IPポートの「3001番」と「3002番」を用意し、認証プログラム204または中継サービスプログラム201からの接続を待つ（ステップ602）。

【0052】次に、接続元が認証プログラム204か、中継サービスプログラム201かをチェックする（ステップ603）。接続元が認証プログラム204であった場合、ユーザが入力した「ユーザ名称」502と「パスワード」503、クライアントプログラム（健康管理システム）203が使用する中継サービスプログラム201のTCP/IPポート番号を受信する（ステップ604）。

【0053】その後、受信したユーザ名称502とパスワード503とが、ユーザDB207のファイルから読み込んだユーザ名称とパスワードの群の中にあるかどうかをチェックする（ステップ605）。もし、群の中になかった場合は、認証プログラム204に「NG」を送信し（ステップ606）、ステップ602からの処理を繰り返す。

【0054】もし、群の中にあった場合は、乱数を使用し、今回の接続に対する固有の暗号鍵を生成し、中継サービスプログラム201のポート番号とともにメモリ中に保持しておき、認証プログラム204に「OK」を送信し（ステップ607）、ステップ602からの処理を繰り返す。

【0055】接続元が中継サービスプログラム201であった場合は、まず、中継サービスプログラム201から中継サービス201が使用しているポート番号と中継の開始か終了かを示すフラグを受信する（ステップ608）。

【0056】中継開始の場合は、保持していた中継サービスプログラム201のポート番号と暗号鍵のペアを調べ、対応する暗号鍵を中継サービスプログラム201に送信する（ステップ609、610）。中継終了の場合は、中継サービスプログラム201のポート番号に対応する暗号鍵をメモリ中から破棄し（ステップ611）、ステップ602からの処理を繰り返す。

【0057】図7は、クライアントコンピュータ2上で稼動する中継サービスプログラム201の動作を示すフローチャートである。

【0058】クライアントコンピュータ2上で稼動する中継サービスプログラム201は、複数の中継用のTCP/IPポートを用意し、クライアントプログラム（健康管理システム）203からの接続を待つ（ステップ701）。

【0059】クライアントプログラム（健康管理システム）203から接続されると、認証サービスプログラム202に接続し、ポート番号と中継開始のフラグを認証サービスプログラム202に送信する（ステップ702）。

【0060】次に、認証サービスプログラム202から暗号鍵を受信する（ステップ703）。

【0061】次に、サーバコンピュータ1上の中継サービスプログラム205と接続し、中継サービス固有の鍵で認証サービスプログラム202から受信した暗号鍵を暗号化して送信する（ステップ704）。

【0062】次に、クライアントプログラム（健康管理システム）203またはサーバコンピュータ1上の中継サービスプログラム205からデータが送信されてくるのを待つ（ステップ705）。

【0063】クライアントプログラム（健康管理システム）203からデータを受信した場合は、その受信したデータが「送信終了」のデータであるかどうかをチェックする（ステップ706）。

【0064】「送信終了」であれば、再度、認証サービスプログラム202に接続して中継用のポート番号と中継終了用のフラグを送信した後、クライアントプログラム（健康管理システム）203とサーバコンピュータ1上の中継サービスプログラム205との接続を切断し（ステップ707）、ステップ701からの処理を繰り返す。

【0065】受信データが通常のデータであれば、そのデータを暗号鍵で暗号化し、サーバコンピュータ1の中継サービスプログラム205に送信し（ステップ708）、ステップ705からの処理を繰り返す。

【0066】サーバコンピュータ1上で稼動する中継サービスプログラム205からデータを受信した場合は、そのデータを暗号鍵で復号し、クライアントプログラム（健康管理システム）203に送信し（ステップ709）、ステップ705からの処理を繰り返す。

【0067】図8は、サーバコンピュータ1上で稼動する中継サービスプログラム205の動作を示すフローチャートである。

【0068】サーバコンピュータ1上で稼動する中継サービスプログラム205は、複数の中継用のTCP/IPポートを用意し、クライアントコンピュータ2上で稼動する中継サービスプログラム201からの接続を待つ（ステップ801）。

【0069】クライアントコンピュータ2で稼動する中継サービスプログラム201から接続されると、まず、暗号鍵を受信し、その暗号鍵を中継サービス固有の鍵で復号してメモリ中に保持しておく（ステップ802）。

【0070】次に、サーバプログラム206と接続し（ステップ803）、サーバプログラム206またはクライアントコンピュータ1上の中継サービスプログラム201からデータが送信されてくるのを待つ（ステップ804）。

【0071】クライアントコンピュータ2上で稼動する中継サービスプログラム201からデータを受信した場合は、その受信したデータが「通信終了」のデータかど

うかをチェックする(ステップ805)。「通信終了」のデータであれば、サーバプログラム206とクライアントコンピュータ2上の中継サービスプログラム201との接続を切断し(ステップ806)、ステップ8701からの処理を繰り返す。

【0072】受信したデータが通常のデータであれば、そのデータをステップ802で入手した暗号鍵で復号し、サーバプログラム206に送信し(ステップ807)、ステップ804からの処理を繰り返す。

【0073】サーバプログラム206からデータを受信した場合は、そのデータをステップ802で入手した暗号鍵で暗号化し、クライアントコンピュータ1上で稼働する中継サービスプログラム201に送信し(ステップ708)、ステップ804からの処理を繰り返す。

【0074】このように、本実施形態によれば、サーバコンピュータ1およびクライアントコンピュータ2に中継サービスプログラム201、202を組み込み、この中継サービスプログラム201、202によって両コンピュータ間のデータを暗号化して通信するようにしているため、ネットワークがバス形式であっても、既設のクライアントプログラム203やオペレーティングシステムに全く変更を加えることなく、ネットワーク3を経由したデータのセキュリティを確保することができる。

【0075】また、中継サービスプログラム201、202は、起動プログラムによって稼働状態と非稼働状態に任意に切替えることができるため、非稼働状態にしておくことにより、暗号化しないデータを送受信することもできる。

【0076】さらに、中継サービスプログラム201、202は、フロッピーディスクやCD-ROM等の記録媒体に記録されてユーザに提供されるため、ユーザは所有するコンピュータ内にハードウェア空間が残っていても、中継サービスプログラム201、202をメモリ内に組み込むのみの操作で、既設のアプリケーションプログラムやオペレーティングシステムを全く変更することなく、暗号化したデータを送受信することが可能になる。

【0077】さらに、本実施形態では、認証サービスプログラム202を設け、クライアントコンピュータ2を使用するユーザの認証を個人単位で行い、かつ個人単位の暗号鍵を生成し、その個人単位の暗号鍵によってデータを暗号化して送信しているため、クライアントコンピュータ2を使用する複数のユーザ間でもデータのセキュリティを確保することができる。

【0078】なお、図1においては、サーバコンピュータ1とクライアントコンピュータ2との間でのデータ通信について説明したが、本発明はこれに限定されるものではなく、図9に示すように、ネットワーク3に接続された複数のパーソナルコンピュータ(PC)91、92、携帯型の情報家電(情報端末)93、94、ワーク

ステーション95の中に組み込んで使用することができる。

【0079】また、認証サービスプログラム202は、必要に応じて付加するようにしてもよい。

【0080】さらに、クライアントコンピュータ2とサーバコンピュータ1間の通信は必ず中継サービスプログラム201、205を経由するため、各コンピュータ間で通信されるデータに関してログをとるようにしてもよい。

【0081】また、個人単位の暗号鍵で暗号化する際の暗号アルゴリズムを、健康管理システム、社員検索システムなどのクライアントプログラム別に異ならせる、あるいはユーザ別に異ならせ、高度のセキュリティを必要とするもの程、復号が困難になるようにしてもよい。

【0082】

【発明の効果】以上説明したように本発明によれば、データを通信するコンピュータ内に中継サービスプログラムを組み込み、この中継サービスプログラムによって他のコンピュータとの間で送受信するデータを暗号化するようにしているため、ネットワークがバス形式であっても、既設のアプリケーションプログラムやオペレーティングシステムに全く変更を加えることなく、ネットワークを経由したデータのセキュリティを確保することができる。

【0083】また、中継サービスプログラムは、起動プログラムによって稼働状態と非稼働状態に任意に切替えることができるため、非稼働状態にしておくことにより、暗号化しないデータを送受信することもできる。

【0084】さらに、中継サービスプログラムは、フロッピーディスクやCD-ROM等の記録媒体に記録されてユーザに提供されるため、ユーザは所有するコンピュータ内にハードウェア空間が残っていても、中継サービスプログラムをメモリ内に組み込むのみの操作で、既設のアプリケーションプログラムやオペレーティングシステムを全く変更することなく、暗号化したデータを送受信することが可能になる。

【0085】さらに、認証サービスプログラムを組み込み、ユーザの認証を個人単位で行い、かつ個人単位の暗号鍵を生成し、その個人単位の暗号鍵によってデータを暗号化して送信するように構成した場合には、同じコンピュータを使用する複数のユーザ間でもデータのセキュリティを確保することができる。

【図面の簡単な説明】

【図1】本発明を適用した暗号化データ通信システムの実施形態を示すシステム構成図である。

【図2】図1の実施形態における中継サービスプログラムを利用した通信時のデータの流れを示す図である。

【図3】クライアントコンピュータに組み込まれた認証プログラムの処理手順を示すフローチャートである。

【図4】認証プログラムが表示するシステム選択画面の



例を示す説明図である。

【図5】認証プログラムが表示するユーザ名称等の入力画面の例を示す説明図である。

【図6】クライアントコンピュータに組み込まれた認証サービスプログラムの処理手順を示すフローチャートである。

【図7】クライアントコンピュータ上で稼動する中継サービスプログラムの処理手順を示すフローチャートである。

【図8】サーバコンピュータ上で稼動する中継サービス

プログラムの処理手順を示すフローチャートである。

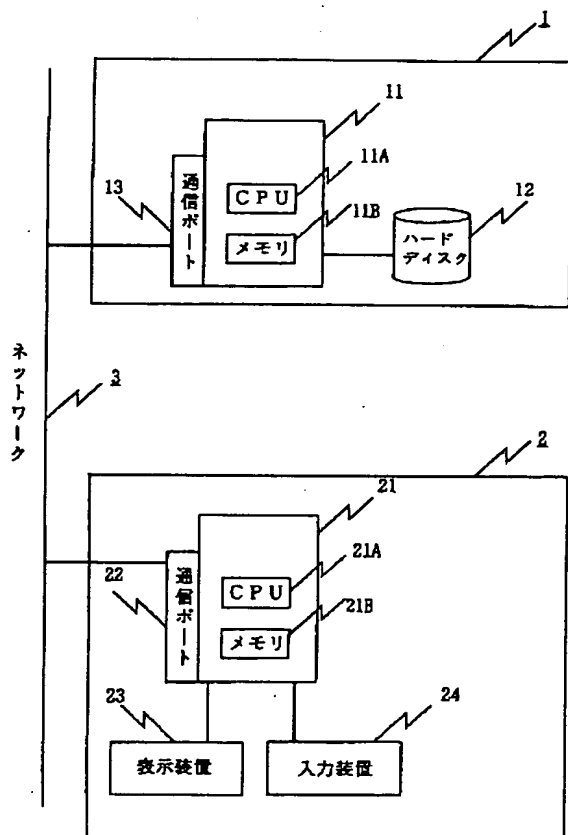
【図9】本発明の適用するコンピュータの他の例を示すネットワーク構成図である。

【符号の説明】

1…サーバコンピュータ、11…端末装置、11A…CPU、11B…メモリ、12…ハードディスク、13…通信ポート、2…クライアントコンピュータ、21…端末装置、21A…CPU、21B…メモリ、22…ハードディスク、23…通信ポート、24…表示装置、25…入力装置、3…ネットワーク。

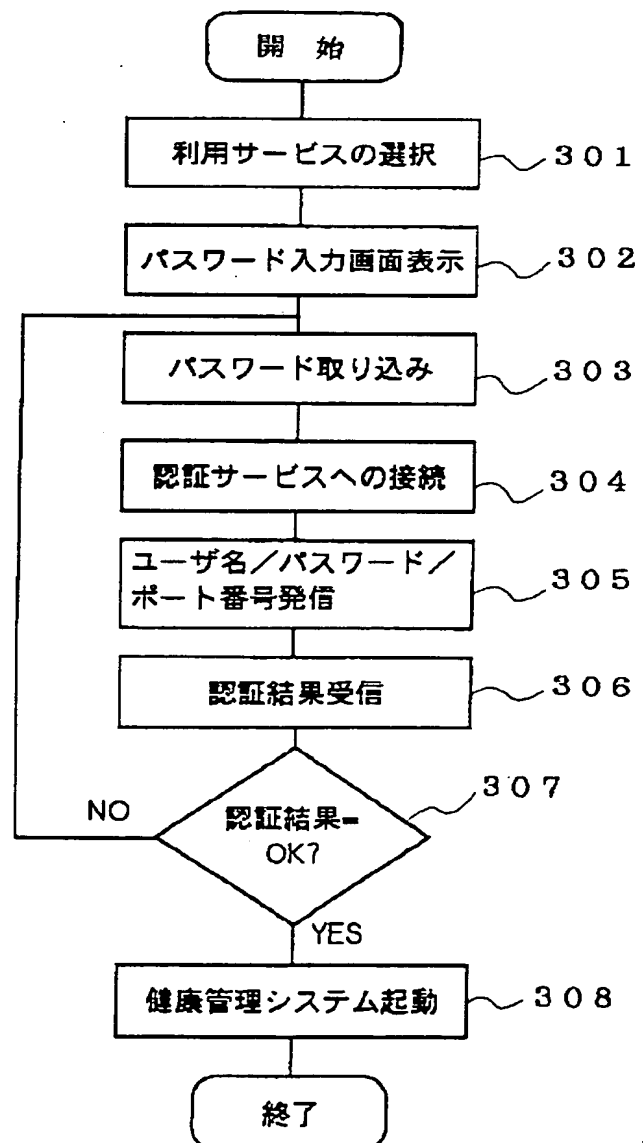
【図1】

図 1

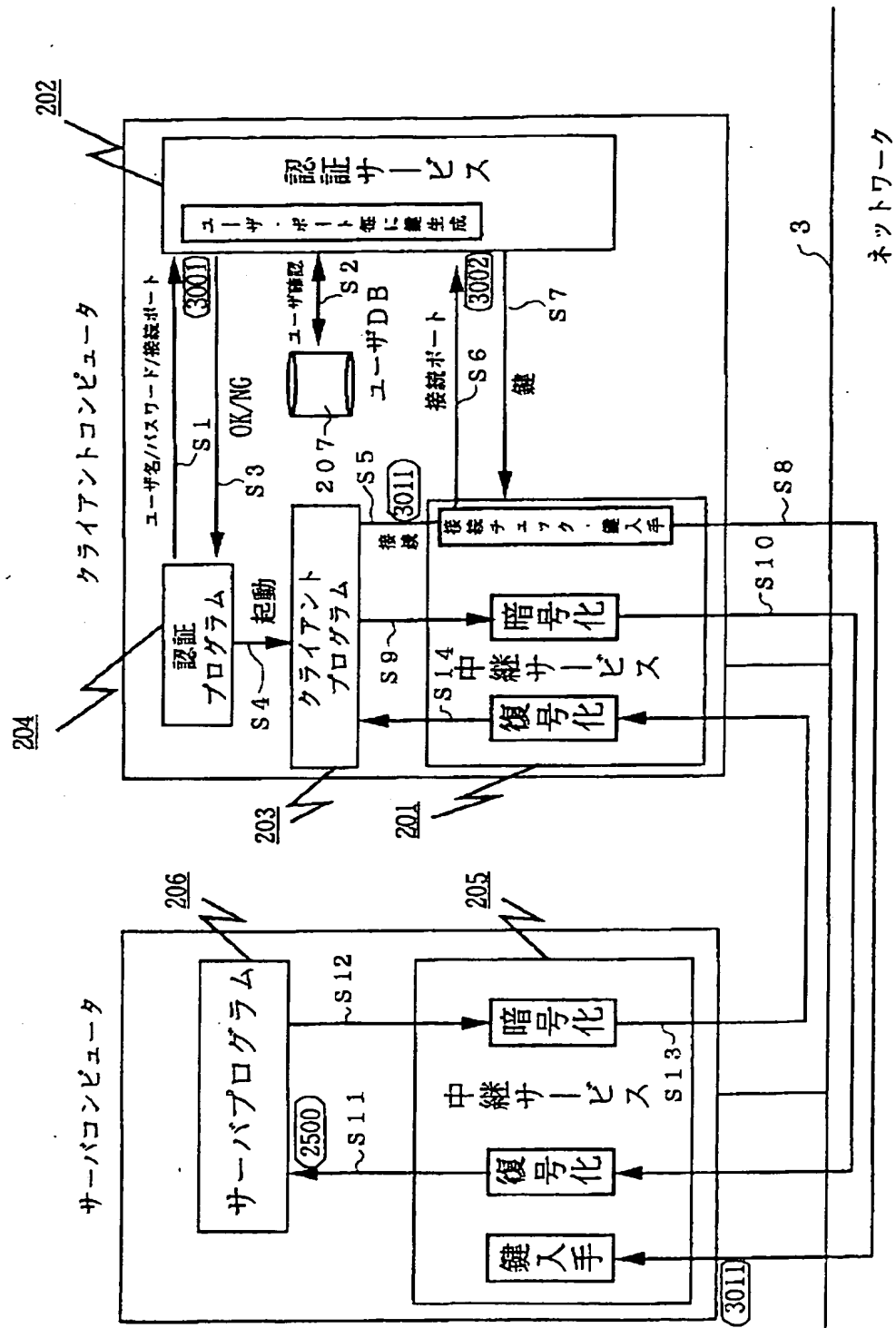


【図3】

図 3

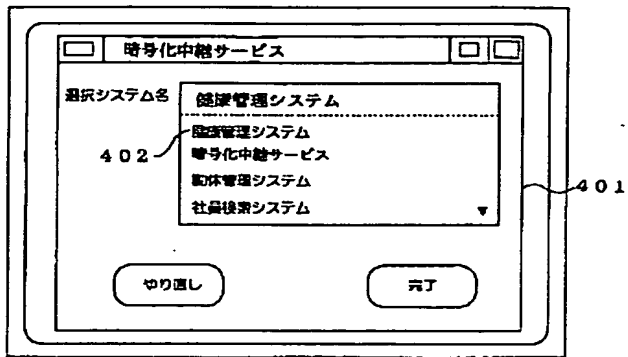


2  
☒



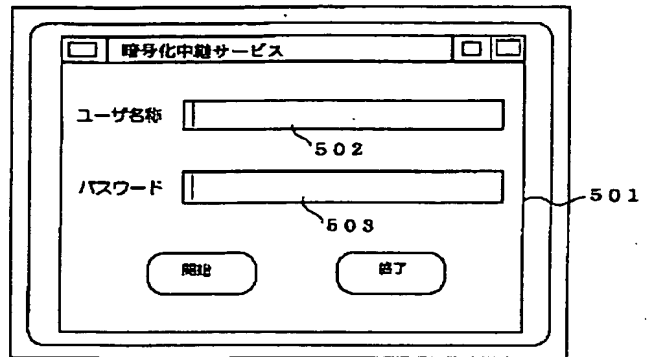
【図 4】

図 4



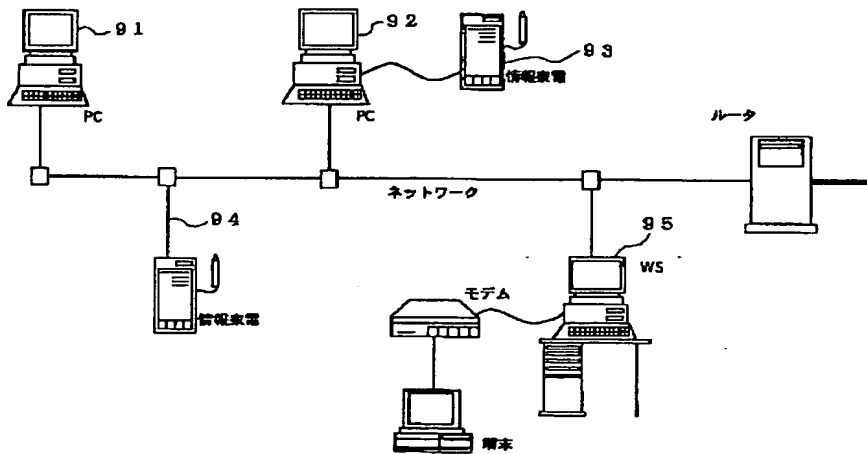
【図 5】

図 5



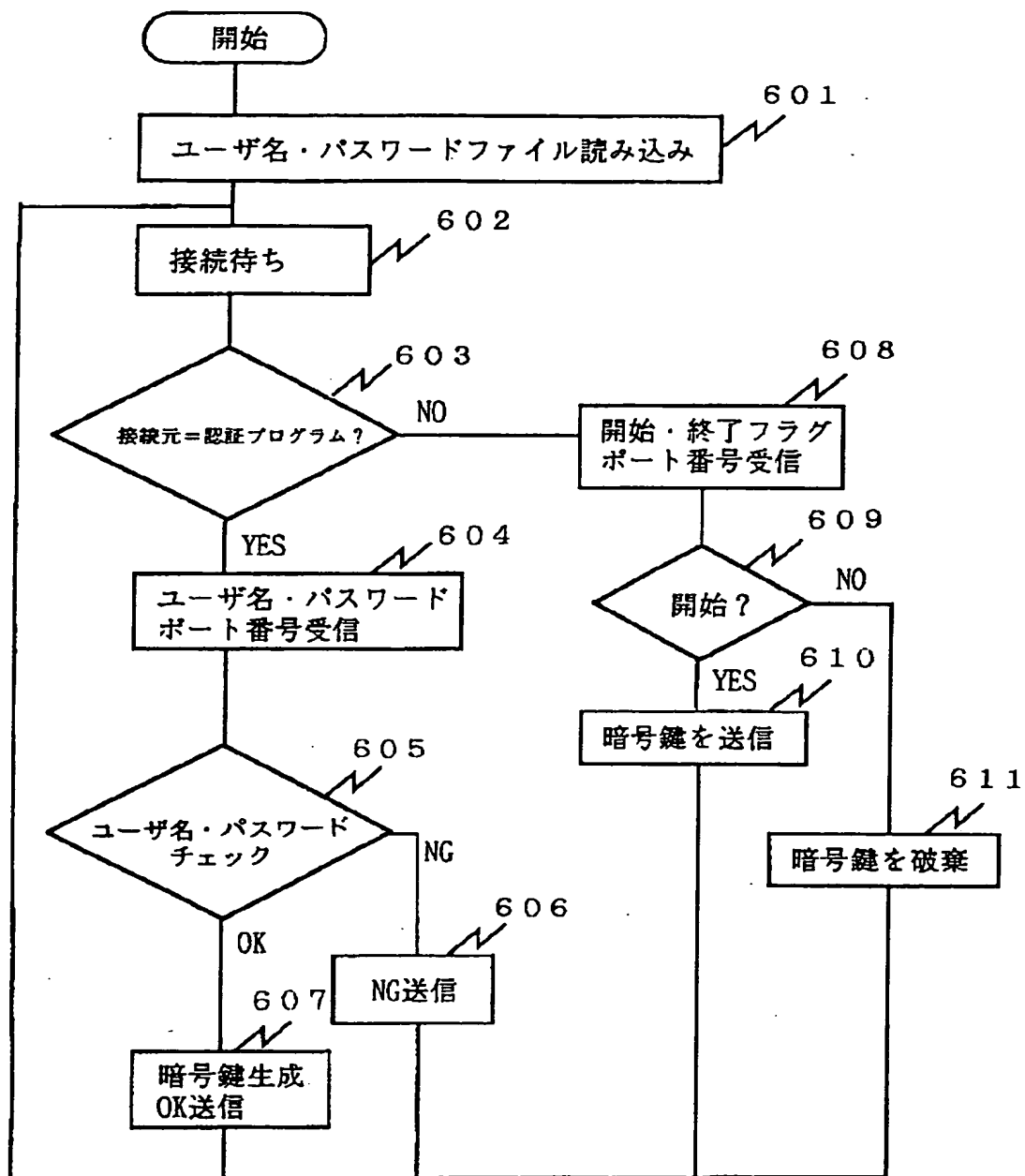
【図 9】

図 9



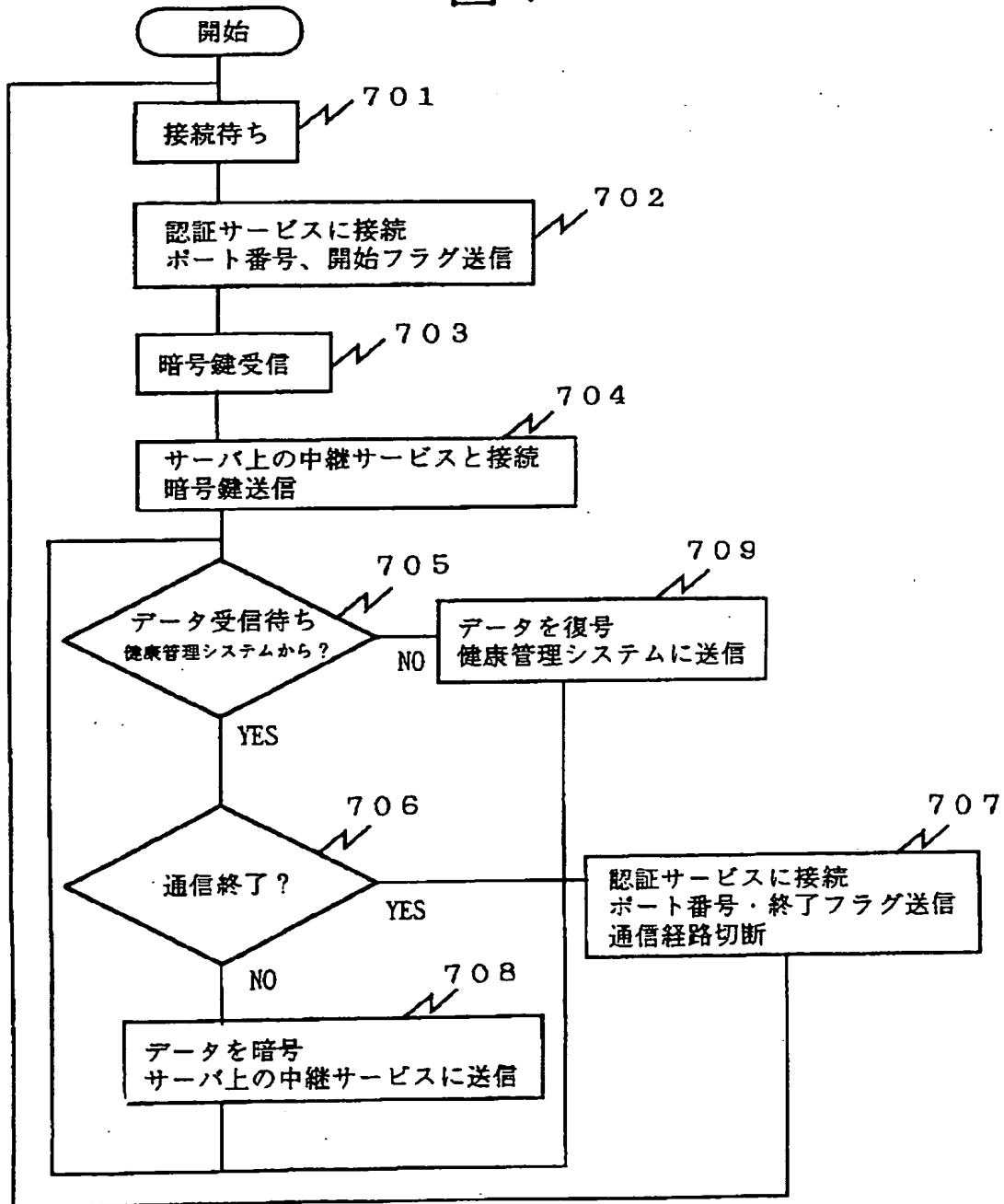
【図6】

図 6



【図7】

図7



【図8】

図 8

